

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, <i>et al.</i> ,	:	
	:	
	:	
Plaintiffs,	:	
	:	
	:	
v.	:	CIVIL ACTION NO.
	:	1:17-CV-2989-AT
BRAD RAFFENSPERGER, <i>et al.</i> ,	:	
	:	
	:	
Defendants.	:	

ORDER

This matter is before the Court on the parties' discovery dispute statements [Docs. 416, 429, 440, 441, 451, 453, 455, 456] regarding Plaintiffs' discovery requests relating to the State's GEMS databases.¹

I. BACKGROUND

Plaintiffs request that the State produce electronic copies of the GEMS databases for the November 6, 2018 election, including both the election configuration version sent to each Georgia county prior to an election and the completed version the counties sent back after the election to the Secretary of State, as well as passwords necessary to access the databases.² The State

¹ Plaintiffs have also separately requested that the State Defendants produce a forensic image of the GEMS server. However, Plaintiffs indicated they wish to first proceed with discovery of the GEMS databases.

² The parties agree that there are multiple GEMS databases. As used in this Order, the term "GEMS database" or "GEMS databases" refers to both the election configuration versions of the

Defendants object to the request based on the assertion that disclosure of sensitive and secure information in the GEMS databases could jeopardize election system security. The State asserts the GEMS databases are protected and carefully guarded as a matter of state law.³ *See* O.C.G.A. §§ 21-2-379.24(g); O.C.G.A. § 21-2-500; *Smith v. Dekalb Cnty.*, 654 S.E. 2d 469 (Ga. Ct. App. 2007). Defendants further contend that any review of information from the GEMS databases must be limited to Plaintiffs' attorneys and their experts and should not be disclosed to any of the Plaintiff-parties in this case.

Plaintiffs seek unrestricted access to the GEMS databases because, they contend, the databases – which are public records in some other states – do not contain any confidential information and their disclosure would not compromise election security. In addition, the Curling Plaintiffs' Request for Production No. 15 seeks underlying data from the GEMS databases. (*See* Doc. 420-1 at 19.) The State Defendants acknowledge that certain data contained in the GEMS databases “is [a] public record.” *Coalition for Good Governance v. Crittenden*, No. 2018-cv-313418, Hr’g Tr. 88:22-24 Jan. 9, 2019 (Ga. Superior Ct. 2019). Counsel for the State Defendants in this case, Vincent Russo, made this representation to Superior Court Judge Adele Grubbs in an election challenge filed in the Fulton County Superior Court in *Coalition for Good Governance v. Crittenden*, Case No. 2018-

GEMS databases sent by the Secretary of State to each Georgia county prior to the November 2018 election and the completed version the counties sent back to the Secretary of State after the election.

³ The State Defendants also contend that Georgia’s GEMS databases “are unique to the state of Georgia – which runs a version not used in any other state.” (Doc. 416 at 4.)

cv-313418 in which he also served as counsel for the Secretary of State. Mr. Russo further stated, “[w]e can pull the data from the GEMS machines to give to them.” *Id.* at 90.⁴

But according to the State Defendants, disclosure of the GEMS databases themselves would reveal the “structure” or “architecture” of Georgia’s election system, providing a roadmap for hackers to infect the system with malware. Instead, as a substitute for the production of the GEMS databases the State Defendants offered to produce documents generated by the GEMS databases that do not reveal the system’s structure, including (1) various reports from the database, (2) “GEMS Verify” tests to compare the executable files to a trusted version, and (3) a list of any macros within the database where any malicious code would appear. The State Defendants have not presented the Court with any testimony from its technology representatives to explain precisely how these documents will allow for the extensive examination Plaintiffs seek to perform. Nor have the State Defendants presented the Court with any testimony from these individuals to explain precisely how providing Plaintiffs’ attorneys and experts with an electronic copy of the GEMS databases, subject to the terms of a confidentiality protective order, would risk disclosure of the GEMS system’s architecture to third-party criminal hacking.

⁴ To date, however, the State Defendants do not appear to have provided this “public” data from the GEMS databases in response to Plaintiffs’ outstanding discovery requests.

Plaintiffs' counsel and their experts, on the other hand, have filed detailed affidavits explaining how the limited discovery the State Defendants are willing to produce is inadequate. According to Plaintiffs' experts Dr. Alex Halderman and Matthew Bernhard, detailed information about the structure and operation of the GEMS database has already been made publicly available:

Several states make their GEMS databases public, as a matter of transparency. The GEMS software itself has been available for download from the website BlackBoxVoting.org for more than 13 years, along with abundant technical documentation about the program.

Defendants assert that the “structure” of Georgia’s GEMS database is unique to Georgia, and that its disclosure would therefore aid attackers. This reflects a misunderstanding of how election-specific malware can operate. Malware does not need to be hard-coded for a specific race ID code or candidate number (which might be unique to a particular state). Instead it can be programmed to search for the name of a candidate or political party, regardless of how that candidate or party is coded in the database. In any event, files that appear to be GEMS databases from certain past elections in Georgia have long been available online at <http://blackboxvoting.org/docs/diebold/marks-gems-files.zip>. If there are characteristics that are unique to all GEMS databases used in Georgia, those characteristics are likely already ascertainable by attackers through analysis of these publicly available files.

(Doc. 441 at 440-41, Decl. of Alex Halderman ¶¶ 3-4; *see also* Doc. 441 at 199, Decl. of Matthew Bernhard ¶ 12 (“The structure of the database is disclosed in GEMS manuals that have been publicly available since the system was first put in service.”))⁵

⁵ Merle King, the former Executive Director of Georgia’s Center for Election Security in his capacity as an expert for the government in Pima County Arizona, testified that “[t]he structure of the database is consistent through all jurisdictions that use GEMS, so the revelation of one jurisdiction’s database structure reveals information – potentially reveals information about

According to the Coalition Plaintiffs' expert Matthew Bernhard, the GEMS reports the State Defendants propose as a replacement for a full examination of the GEMS database may not report all errors in the GEMS system:

The tables in the GEMS database store a variety of information about an election, including candidate names and party affiliation, jurisdictions, information about the voter access cards, ballot styles, how election results should be reported, precincts, polling locations, ballots layout, and so on. At the conclusion of the election, results are also written into the database, including how many votes were cast on each machine in each precinct, how many votes were cast for each candidate, the number of write-in votes, and so forth.

An error in the data entry into the GEMS database, such as switching the two identifiers for two candidates, could have an impact on the outcome of an election without being easily detected. Worse, if an error in the database causes a buffer overflow, the error may not be reported in subsequent data reporting mechanisms by the GEMS system, like the system report PDFs that GEMS can generate. The only way to know if there is bad data in the database which might cause unexpected behavior when in use is to examine the database itself.

Some of the data contained within the GEMS database is also present in the reports generated by the GEMS software. [These reports] include:

- Base Precincts with Race Report: an accounting of which races appeared on the ballot in each precinct;
- Vote Center with Cards Report: an accounting of which memory cards and ballot styles were present in each precinct;
- Statement of Votes Cast Report: Election results by precinct for every candidate on the ballot in each precinct;
- Summary Report: summarized election result including breakdowns by type of ballot cast (early voting, absentee by mail, and so on);

other jurisdictions." (Doc. 441 at 90, Deposition of Merle King at 11:17-21.) Mr. King testified that he was concerned about the release of the Pima County, Arizona GEMS database to the public because it would expose the general structure of the GEMS database, which is consistent among jurisdictions, precisely because it could thus reveal information about the GEMS databases used in other jurisdictions. (*Id.*) Ultimately the judge presiding over the Pima County matter ordered release of these GEMS records as public records under Arizona law.

- Ballot Image Report: a text representation of every ballot recorded by the voting system during the election (one report for every ballot cast, i.e. millions of pages of data from just the November 2018 election alone).

These reports fail to provide crucial information contained in the GEMS database. Due to the potential vulnerabilities discussed above, and the fact that these reports are generated by the GEMS database itself, it is entirely possible that errors which reside in the database would not appear in these reports. For example, if a field in the database incidentally triggers a buffer overflow⁶, this error may not appear in the written report.

These reports also do not contain all of the data in the GEMS database that is germane to an inquiry about configuration errors or malware. For example, nothing in the reports would show a miscoding of a candidate's name. Vote totals which were erroneously counted for Candidate A due to a misconfiguration, for example, would also appear that way in the reports. Essentially, the reports do not create an independent evidentiary trail with which to assess the correctness of the GEMS database, because they (a) do not contain all of the data in the database and (b) will not exhibit errors in a detectable way.

Not only do these reports not constitute a faithful recreation of the GEMS database, but they create a significant burden on the investigation. The database is fully searchable and can be examined using standard database tools. GEMS reports are PDFs, which would preclude the usage of tools that could facilitate easy comparison and validation of entries. Examining and testing tabulations on millions of pages of ballots image reports alone would take far more time than a full forensic investigation of the entire GEMS server.

(Doc. 441 at 198-99, Bernhard Decl. ¶¶ 14-15, 18-21.)

Dr. Alex Halderman's affidavit confirms that a review of reports generated by the GEMS software is not a sufficient substitute for an examination of the database itself:

These reports contain only a subset of the information contained in the GEMS database. While the GEMS database is the actual data and

⁶ Mr. Bernhard's explanation of a buffer overflow is provided below.

coding used to operate the election, the reports are merely an approximate translation and summary, rendered into human-readable form by GEMS itself. Like any translation, the reports necessarily omit subtleties and nuances that can affect the meaning of the information. Moreover, since these reports are produced by the GEMS software, errors or malware affecting the GEMS system could cause crucial information to be omitted from the reports.

(Doc. 441 at 442, Halderman Decl. ¶ 6.)

Mr. Bernhard's affidavit further details how defects in the GEMS database can occur without the installation of malicious software:

Because certain data types in the database can have arbitrary length, if a program is reading from the database and does not properly account for the length of the data, it may accidentally read so much data that it overwrites its own program. This is what is known as a *buffer overflow* (a *buffer* is where data is kept when it is being read out of a file or database). Overflows may occur due to incorrect lengths being specified in the database, improperly formatted character sequences, or simply data that is unexpectedly long. A clever attacker can craft data that, when the program reads the data in, results in a buffer overflow and overwrites the original program with code that the attacker wrote. This is a buffer overflow attack, or an exploitation of a buffer overflow, and it is one of the most common ways that hackers gain unauthorized access to systems.

Even though the data in the database is not treated as code that can be executed by a computer, if the data overwrites a piece of the program that is reading the data it will be executed by the computer as if it were part of the program. Even in the absence of malicious intent, a buffer overflow vulnerability can result in unexpected or undetected behavior by a program.

(Doc. 441 at 198, Bernhard Decl. ¶¶ 8-9.)

Finally, Mr. Bernhard explains that a review of the macros list (suggested by the State as an alternative to the GEMS database) will not necessarily indicate the presence of a malware or other defects in the database:

Another common threat vector for database programs (in particular Microsoft Access) is the use of macros, which are small programs that can be written inside the database program to assist in arduous or repetitive tasks. These macros, while powerful, also present a major security vulnerability to most database engines, as malicious macros can take over the database software and corrupt data.

However, even if macros are entirely disabled, if data in the database is not formatted in a way that the program reading it expects, it can still lead to a buffer overflow. Regardless of whether macros are enabled or not, data that exists in the database can still result in unexpected or malicious behavior to occur in the program that is reading the data.

(Doc. 441 at 199, Bernhard Decl. ¶¶ 10-11.)

As this Court indicated in its July 2, 2019 Order, an analysis of the GEMS databases is highly relevant to Plaintiffs' claims, as Plaintiffs' experts contend that such an analysis is a necessary first step in evaluating security vulnerabilities and flaws in the State's GEMS system which have an actual impact on voting tabulations. Thus, to strike a balance between the State Defendants' security concerns and the Plaintiffs' need for access to the GEMS database for examination, the Court proposed that the State Defendants provide Plaintiffs a mirror image of the GEMS database on a secure computer at the Secretary of State's secure facility.

In response to the Court's suggestion, the State submitted the following proposal for a review of the GEMS databases at the Secretary of State's offices:

The Secretary of State's office will:

1. Create a server image with the same environment used in the counties, which will remain in a secure, air-gapped environment.
2. Load a copy of the GEMS Database from the November 2018 election.

3. Install Microsoft Access on the computer.
4. Remove the GEMS Application.
5. Allow Plaintiffs' expert to have supervised access in the Secretary of State's facility.
6. Plaintiffs will not be permitted to introduce any software or files onto the computer and will not be permitted to connect any hardware to the computer.
7. Plaintiffs will not be permitted to remove any files from the computer.
8. Plaintiffs will not be permitted to take pictures or videos of their review process.
9. Plaintiffs must make copies of all notes taken during the review and leave a copy of those notes with the Secretary of State's office except for attorney work product.

(Doc. 440 at 4-5.)

As a number of the State's conditions potentially appeared as too restrictive to afford a meaningful review of the information in the GEMS databases, the Court directed Plaintiffs to identify what conditions, if any, they contend will severely impair their ability to perform the necessary examination of the information in the databases and their proposed alternatives.

Although the Court understood Plaintiffs to be initially receptive to the Court's proposal during the June 29, 2019 telephone conference regarding this dispute, Plaintiffs' counsel have subsequently objected to the proposal as being entirely unnecessary and unduly burdensome. First, Plaintiffs insist that the

GEMS database should be produced immediately without restriction on a CD and should not be subject to any security protocols because it is not confidential.

Second, Plaintiffs assert that: (i) it is not reasonable or necessary to require Plaintiffs' attorneys and experts to travel hundreds of miles to Atlanta to review the GEMS databases in Defendants' facilities; (ii) this restriction would make review of the GEMS databases prohibitively expensive, logically difficult, and unnecessarily time consuming given that review of the databases will take many days and potentially weeks; (iii) Plaintiffs' representatives will need to go back to the data again and compare it to other data and documents to get a full picture of the issues inherent in the system; (iv) the proposed access conditions would severely impede an effective examination because the State proposes to provide a single computer using obsolete versions of Microsoft Windows, rather than the use of more modern secure software; (v) Plaintiffs' experts and attorneys must be able to install appropriate software and data to protected PCs to conduct their analysis of the GEMS databases, such as specialized software to examine the low-level structure of the databases, to compare multiple versions of the databases, to check the data for consistency, and a review of the GEMS databases without the necessary tools would not allow the detection of errors, vulnerabilities, and viruses that are potentially hidden in the databases; (vi) Plaintiffs need a team of attorneys, experts, and support staff to review the GEMS databases given the volume of data, it is not possible for two cybersecurity experts to conduct this review alone, as it is likely to take weeks of effort by a team of people; and (vii) Plaintiffs' attorneys and

experts must be able to take and retain notes that are never shared with Defendants and to privately confer in order to develop and test hypotheses about the data. (*See* Doc. 451-2, Halderman Decl. ¶¶ 9-11.) Alternatively, Plaintiffs propose that their review of the databases be allowed to take place on secure computers in their own facilities subject to a security protocol outlined by Dr. Halderman and an additional regime of security protocols overseen by John Carlin, former Assistant Attorney General for the U.S. Department of Justice's National Security Division and former Chief of Staff to Robert S. Mueller, III, who is counsel of record for the Curling Plaintiffs. (*See* Doc. 451; Halderman Decl.; Declaration of David Cross ¶¶ 2-4.)

In response to Plaintiffs' objections⁷, the State modified its proposal as follows:

1. Create a server images on computers which will remain in a secure, air-gapped environment. State Defendants will make six computers with Windows 10, Microsoft Access 2019, and Microsoft Excel 2019 available to Plaintiffs' experts and their assistants.
2. Load a copy of the GEMS Databases⁶ from the November 2018 election.
3. Install Microsoft Access and Microsoft Excel.
4. Remove the GEMS Application.

⁷ This Court ordered the State to supplement its response to include (1) the number of computers the Secretary of State's Office would be prepared to make available for Plaintiffs' experts to conduct database reviews and work on; and (2) the size (i.e., dimensions) of the work space that would be made available to accommodate Plaintiffs' experts and their assistants as they work; and (3) the maximum length of time that such space and computers would be made available. (*See* July 8, 2019 Order by docket entry only.)

5. Allow Plaintiffs' experts and attorneys to have supervised access in the Secretary of State's facility. State Defendants will provide a room currently used for training up to 25 people, with dimensions of 18 feet by 30 feet in the Secretary of State's facility. State Defendants will provide the space for five business days from 8:00 a.m. to 5:00 p.m.
6. Plaintiffs will only be permitted to introduce any software or files onto the computer that have been reviewed and approved the Secretary of State's IT Department. If there is a dispute about whether a particular software is needed to facilitate a review, Plaintiffs may present that dispute to the Court.
7. Plaintiffs will not be permitted to connect any hardware to the computer.
8. Plaintiffs will not be permitted to remove any files from the computer. The Secretary of State's office will extract any data files Plaintiffs believe are required as long as those files contain only data and no confidential information and will provide those to Plaintiffs.
9. Plaintiffs will not be permitted to take pictures or videos of their review process.
10. Plaintiffs must make copies of all notes taken during the review and leave a copy of those notes with the Secretary of State's office except for attorney work product.

(See Docs. 453 and 456.)

II. ANALYSIS

The Court recognizes the centrality of the Plaintiffs' experts' analysis of the functionality and accuracy of the GEMS database to the Plaintiffs' constitutional claims in this case and the significance of accuracy of voting count concerns. This was clearly manifested in the evidence presented and the Court's original order on

the preliminary injunction issued on September 17, 2018. (Doc. 309.) The Court has also consistently recognized that the State retains an essential interest in protecting the integrity of the election system and the confidentiality of the functioning of the election data system.

The Court had originally been hopeful that an appropriate balance could be struck between the parties' respective interests by fashioning a working arrangement for Plaintiffs' counsel and their experts review and analysis of the requested November 2018 GEMS databases at the Secretary of State's information technology secure offices and with the crafting of appropriate confidentiality provisions. After considered review of the extensive back and forth submissions from the parties as well as a substantive discovery phone conference with counsel and their respective experts, the Court concludes that the State Defendants have ultimately not provided practical or reasonable terms for the Plaintiffs' experts' review and analysis of the GEMS databases. The terms insisted upon by the State Defendants would in reality preclude Plaintiffs' experts from effectively analyzing the database and its functioning as well as preclude Plaintiffs' experts from collecting in writing any of their observations on a real time basis during their review. The State's proposed procedures impose time restrictions for access to the Secretary of State's offices for review of the data that are not consistent with the fast track of litigation in this case, the complexity of the analysis to be performed, and the imminence of a preliminary injunction hearing. Finally, the State's proposed procedures would vitiate a whole portion of Plaintiffs' counsel's work

product privilege if they were to accompany their experts to review the database in the Secretary of State's information technology office. In sum, if the Court were to proceed with the State's proposed procedures, it would effectively be cutting off the Plaintiffs' capacity to investigate and present their claims with competent, requisite expert testimony, despite their strong showing of an institutional capacity to maintain the highest level of confidential protective measures.

Plaintiffs have agreed to and are prepared to implement an array of confidentiality protective procedures at two reliable entities (the University of Michigan in Ann Arbor, under the supervision of Dr. Alex Halderman and Morrison & Foerster in Washington, D.C., under the supervision of counsel, including the former Assistant Attorney General for the U.S. Department of Justice's National Security Division) with well established institutional expertise in the management of high level security for sensitive, confidential information technology and databases. (*See Doc. 451 and attachments; Doc. 455*).

Georgia law does not recognize as public records sensitive voting database and voting system information the release of which might endanger election security. *See O.C.G.A. §§ 21-2-379.24(g)* ("*Documents or information* that, if made public, would *endanger the security of any voting system* used or being considered for use in this state, or any component thereof, including, but not limited to, electronic ballot markers, DREs, ballot scanners, pollbooks, and software or databases used for voter registration, *shall not be open for public inspection* except upon order of a court of competent jurisdiction.") (emphasis

added); O.C.G.A. § 21-2-500 (providing voting machine ballot labels, computer chips containing ballot tabulation programs, copies of computer records of ballot design, and similar items or an electronic record of the program by which votes are to be recorded or tabulated *shall be stored under seal* for at least 24 months, after which time they shall be presented to the grand jury for inspection, and upon the adjournment of the grand jury they may be destroyed, unless otherwise provided by order of the superior court) (emphasis added); *Smith v. Dekalb Cnty.*, 654 S.E. 2d at 470, 472 (holding that Georgia citizen was not entitled under Georgia Open Records Act to a copy of “the GEMS CD–ROMS” containing “a copy of the information on each memory card (PCMCIA Card) which shall include all ballot images and ballot styles as well as vote totals and a copy of the consolidated returns from the election management system” because the CD-ROM “was statutorily designated to be kept under seal, it is by law prohibited or specifically exempted from being open to inspection by the general public and, therefore, is not an open record subject to disclosure”). However, Georgia does recognize that such information may be released upon order of a court of competent jurisdiction. O.C.G.A. § 21-2-379.24 (g). In other words, even if the Court accepts the State’s view that the GEMS database is highly sensitive (though such databases not treated similarly by many other states which classify the database as a public record and although GEMS database records are made available by multiple Georgia counties), the Court does not view the confidentiality protection asserted here by the State as an absolute privilege. This is made all the more so true in the context

of a federal lawsuit involving constitutional claims directed at the security and integrity of the voting process and tabulation itself and where Plaintiffs' counsel and their experts are prepared to implement appropriate, strong security measures.

Based upon the Court's familiarity with this case and its assessment of the evidence, briefs, case management, and legal considerations before it, the Court finds that release of the 2018 GEMS database (pre and post November election) to Plaintiffs' two designated experts and counsel, subject to the protective confidentiality and security provisions specified below, is appropriate and is hereby **ORDERED**.

III. ORDER ON DISCOVERY OF GEMS DATABASES

For the foregoing reasons, the Court finds that the following discovery and disclosure provisions are appropriate.

The State Defendants will produce to Plaintiffs' experts and counsel copies of the GEMS databases⁸ on a CD or other appropriate electronic media in a form readable by Microsoft Access or other standard database format for analysis by the Plaintiffs' experts⁹ and attorneys. Defendants are **DIRECTED** to either (1) arrange for delivery either by courier / express mail service to Dr. Halderman at the University of Michigan (Ann Arbor) and David Cross or John Carlin at

⁸ As explained above, the term "GEMS database" or "GEMS databases" refers to both the election configuration versions of the GEMS databases sent to each Georgia county prior to the November 2018 election and the completed version the counties sent back after the election to the Secretary of State.

⁹ Plaintiffs' experts referenced are Dr. Alex Halderman and Matthew Bernhard.

Morrison & Foerster in Washington D.C.; or, (2) arrange for designated representative(s) of the Secretary of State's office to personally deliver the requested GEMS databases to each of the identified locations and representatives above. Delivery shall be made no later than 2:00 pm on Friday, July 12, 2019. Plaintiffs shall be responsible for reimbursement to the State Defendants of all courier or airline travel costs incurred.

Plaintiffs' experts and any staff assisting them shall execute confidentiality agreements that recognize their obligations to maintain the confidentiality of the GEMS databases provided, subject to the Court's further rulings in this case as to the scope of information that potentially can be disclosed or the manner of such disclosure.

Plaintiffs' experts and counsel will establish locked, secure designated work rooms at the University of Michigan in Ann Arbor, Michigan and the Washington, D.C. office of Morrison & Foerster LLP in which only Plaintiffs' attorneys and Plaintiffs' experts have access. As the Coalition Plaintiffs' counsel did not make any individual showing as to the security provisions that are already or can immediately be reliably instituted in their Atlanta law office(s), the Coalition Plaintiffs' counsel will be required to access the database at either the University of Michigan or Morrison & Foerster designated facilities.

Plaintiffs' experts will install the GEMS databases onto a limited number of air-gapped, password protected, stand-alone computers ("Protected PCs") that are not connected to the internet and that are located in the locked secure space

described both above and below. The following additional conditions to this authorization and provision are applicable:

- The designated secure areas shall have limited access, by key or key card, only available to experts or attorneys on the review team (i.e., janitorial staff and any others will not have access to the room);
- 24-hour video camera surveillance of the entrances to each of the designated two facilities, and a log of access to the work areas shall be maintained;
- Installation of copies of the GEMS databases onto a maximum of six (6) air-gapped, password-protected, standalone computers that are not connected to the internet (the “Protected PCs”) is authorized, the allocation per facility to be determined by Plaintiffs’ counsel jointly with their experts. Plaintiffs’ experts and attorneys are authorized to install software review tools (via USB sticks) onto the Protected PCs to conduct their review of the GEMS databases on an efficient and accurate basis.

Plaintiffs’ experts and attorneys may bring their own laptops into the secure work areas subject to the following restrictions: (1) GEMS databases shall not be connected to the internet via an external wireless network while they are in the designated work room; (2) Laptops may be connected to the internet via an external wireless network while they are in the room, but they shall not be networked in any fashion or form to any of the Protected PCs on which the GEMS databases are installed; (3) GEMS databases, mirror images of such databases, and videotapes of such shall not be installed on the experts’ or Plaintiffs’ attorneys’ own

laptops. If individual sample screen shots are ultimately later considered necessary for provision of an expert opinion at trial, Plaintiffs shall identify such to Defendants. If the parties cannot agree on terms for production of such, they shall submit the dispute to the Court on a timely basis.

Plaintiffs' experts and attorneys may maintain private notes and communications regarding their review of the GEMS databases that will be maintained as "confidential" attorney work product, subject to the provisions of Rule 26 of the Federal Rules of Civil Procedure and this Order. Protective measures shall be implemented to ensure that strict confidentiality measures are implemented regarding all such notes and communications as well as the storage of any non-connected laptops used for maintaining notes.

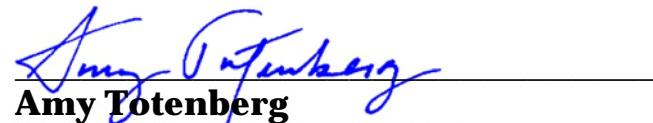
As counsel of record, Plaintiffs' attorneys are individually bound to comply with the confidentiality as well as other security provisions of this Order. Any law firm employee, assistant, or counsel (not of record) participating in this case shall also be required to execute an agreement acknowledging the confidentiality provisions of this Order.¹⁰

In the event the State Defendants deliver the copies of the designated GEMS databases via representative(s), such representatives are authorized to view the

¹⁰ These confidentiality provisions may be modified by further Order of the Court as necessary in the future.

security features of the respective designated facilities at the time of their performing delivery.

IT IS SO ORDERED this 9th day of July, 2019.



Amy Totenberg
United States District Judge